Available online at www.sciencedirect.com
ScienceDirect
Theoretical Computer Science 380 (2007) 115–126
Theoretical Computer Science
www.elsevier.com/locate/tcs

The quantum query complexity of the abelian hidden subgroup problem

Pascal Koiran*, Vincent Nesme, Natacha Portier

Laboratoire de l'Informatique du Parallélisme, École Normale Supérieure de Lyon, 46, allée d'Italie, 69364 Lyon, Cedex 07, France

Abstract

Simon, in his FOCS'94 paper, was the first to show an exponential gap between classical and quantum computation. The problem he dealt with is now part of a well-studied class of problems, the hidden subgroup problems. We study Simon's problem from the point of view of quantum query complexity and give here a first non-trivial lower bound on the query complexity of a hidden subgroup problem, namely Simon's problem. More generally, we give a lower bound which is optimal up to a constant factor for any abelian group.

Keywords: Quantum computing; Query complexity; Lower bounds; Polynomial method; Hidden subgroup problems; Simon's problem

1. Introduction

Given an abelian group G and a subgroup $H \leq G$, a function $f : G \to X$ is said to be hiding H if f can be defined in a one-to-one way on G/H. More precisely, f hides H if and only if

$$\forall g, g' \in G \ \left(f(g) = f(g') \iff \exists h \in H \ g = g' + h\right).$$

Suppose G is a fixed group and f is computed by an oracle: a quantum black-box. We are interested here in algorithms that find the hidden subgroup H. A large amount of documentation about the hidden subgroup problem can be found in the book of Nielsen and Chuang [15].[1] Among all the work already done on such algorithms, one can cite Shor's famous factoring algorithm [19]: this uses a period-finding algorithm, which is a special case of a hidden subgroup problem. In recent years, attention has shifted to non-abelian hidden subgroup problems, but we will restrict our attention here to abelian groups, and in particular to groups of the form $(\mathbb{Z}/p\mathbb{Z})^n$.

In general, two kinds of complexity measures for black-box problems can be distinguished: query complexity, i.e., the number of times the function f is evaluated using the black-box, and computational or time complexity, i.e., the number of elementary operations needed to solve the problem. Typically, a hidden subgroup algorithm is

* Corresponding author. Tel.: +33 72 72 80 00; fax: +33 72 72 80 80.
E-mail addresses: Pascal.Koiran@ens-lyon.fr (P. Koiran), Vincent.Nesme@ens-lyon.fr (V. Nesme), Natacha.Portier@ens-lyon.fr (N. Portier).

[1] History of the problem on page 246 and expression of many problems (order-finding, discrete logarithm...) in terms of hidden subgroup problems on page 241.

0304-3975/$ - see front matter
doi:10.1016/j.tcs.2007.02.057

considered efficient if its complexity (in query or in time, depending on the interest) is polynomial in the logarithm of the cardinality of G. For example, Kuperberg's algorithm [12] for the (non-abelian) dihedral hidden subgroup problem is subexponential (but superpolynomial) in both time and query complexities.

Our main result is that the query complexity of finding a subgroup hidden in G is of the order of magnitude of $r(G)$ for any abelian group G, where $r(G)$ denotes the *rank* of G, that is, the minimal cardinality of a generating set of G (for instance, $r((\mathbb{Z}/p\mathbb{Z})^n) = n$ if $p \geq 2$ is an arbitrary integer). The proof of this result is naturally divided into an upper bound and a lower bound proof. The upper bound is achieved through a tight analysis of the standard Fourier sampling algorithm. It is a folklore theorem in quantum computation that this algorithm solves the hidden subgroup problem in abelian groups with polynomial query complexity (see, for instance, [8,6,2] or [9]), but strangely enough no precise analysis seems to be available in the literature.

The greatest part of this paper is devoted to the lower bound proof. Here all the important ideas already appear in the analysis of Simon's problem, to which our preprint [10] is devoted. It is therefore fitting to recall the history of this problem, which is defined as follows. We are given a function f from $G = (\mathbb{Z}/2\mathbb{Z})^n$ to a known set X of size 2^n, and we are guaranteed that the function fulfils Simon's promises, that is, either:

(1) f is one-to-one, or
(2) $\exists s \neq 0\ \forall w, w' \quad f(w) = f(w') \iff \big(w = w' \vee w = w' + s\big)$.

The problem is to decide whether (1) or (2) holds. Note that (1) is equivalent to "f hides the trivial subgroup $H = \{(0, \ldots, 0)\}$" and (2) is equivalent to "f hides a subgroup $H = \{(0, \ldots, 0), s\}$ of order 2". The original problem [20] was to compute s, and the problem considered here is the associated decision problem. Of course, any lower bound on this problem will imply the same one on Simon's original problem. In his article, Simon shows that his problem can be solved by a quantum algorithm which makes $O(n)$ queries in the worst case and has a bounded probability of error. The time complexity of his algorithm is linear in the time required to solve an $n \times n$ system of linear equations over $(\mathbb{Z}/2\mathbb{Z})^n$. He also shows that any classical (probabilistic) algorithm for his problem must have exponential query complexity. In this paper we shall give a $\Omega(n)$ lower bound on the query complexity of Simon's problem, thus showing that Simon's algorithm is optimal in this respect. Our lower bound applies in fact to groups of the form $(\mathbb{Z}/p\mathbb{Z})^n$, where p is a prime number. The only difference with the special case $p = 2$ treated in our preprint [10] is that the formulas get more complicated. As a side remark, note that Simon also gives a Las Vegas version of his algorithm with expected query complexity $O(n)$. Even better, Brassard and Høyer [4] have given an 'exact polynomial time' quantum algorithm for Simon's problem (i.e., their algorithm has a polynomial worst-case running time and zero probability of error).

The two main methods for proving query complexity lower bounds in quantum computing are the adversary method of Ambainis and the polynomial method (for an excellent review of these methods in French, read [18]). We shall use the polynomial method, which was introduced in quantum complexity theory in [3]. There are recent interesting applications of this method to the collision and element distinctness problem [1,14]. All previous applications of the polynomial method ultimately rely on approximation theory lemmas of Paturi [17] or Nisan and Szegedy [16].

Besides the application to a new type of problems (namely, the hidden subgroup problems), we also contribute to the development of the method by applying it in a situation where these lemmas are not applicable. Instead, we use an apparently new (and elementary) approximation theory result: Lemma 5 from Section 3.

The remainder of this paper is organized follows. After some preliminaries in Section 2, we give in Section 3 an $\Omega(n)$ lower bound for groups of the form $(\mathbb{Z}/p\mathbb{Z})^n$, where p is a prime number. The general case of arbitrary abelian groups (lower and upper bound) is treated in Section 4.

Obtaining tight bounds for non-abelian groups is, of course, a natural open problem. As pointed out at the end of this paper, our results already imply lower bounds for some non-abelian groups, and in particular for the symmetric group $\mathfrak{S}_n$. Additional results on the query complexity of hidden subgroup problems in the *test model* and in the *collision model*, which are weaker query models than the standard query model used in the present paper, can be found in our research report [11].

2. Preliminaries: Definitions and main theorem

From now on, p denotes a prime number and the problem of distinguishing the trivial subgroup from a group of order p in $(\mathbb{Z}/p\mathbb{Z})^n$ will be called 'Simon's problem in $(\mathbb{Z}/p\mathbb{Z})^n$' or sometimes just **Simon's problem**. More

precisely, we are given a function f from $G = (\mathbb{Z}/p\mathbb{Z})^n$ to a known set X of size p^n, and we are guaranteed that **the function fulfils Simon's promises**, that is, either:

(1) f is one-to-one, or
(2) $\exists s \neq 0\ \forall w, w'\ \left[f(w) = f(w') \iff w - w' \in \langle s\rangle\right]$, where $\langle s\rangle$ is the subgroup generated by s.

Again, the problem is to decide whether (1) or (2) holds. As pointed out in the introduction, Simon considered only the case $p = 2$.

We assume here that the reader is familiar with the basic notions of quantum computing [15,7] and we now present the polynomial method. Let A be a quantum algorithm solving Simon's decision problem. Without loss of generality, we may and we will suppose that, for every p and n, the algorithm A acts like a succession of operations

$$U_0^{(p,n)}, O, U_1^{(p,n)}, O, \ldots, O, U_{T(p,n)}^{(p,n)}, M$$

on an m-qubit, for some $m \geq 2n$, starting from state $|0\rangle^{\otimes m}$. The $U_i^{(p,n)}$ are unitary operations independent of f and O is the call to the black-box function: if $x \in G$ and $y \in X$, then $O|x, y, z\rangle = |x, y \oplus f(x), z\rangle$. Here $\oplus$ denotes bitwise addition modulo 2 (we assume that the elements of X are represented by strings of $\lceil p \log n\rceil$ bits). Note that O actually depends on p, n and f. These superscripts are ommited for notational simplicity. The operation M is the measure of the last qubit. There are some states of $(m-1)$-qubits $|\phi_0(p, n, f)\rangle$ and $|\phi_1(p, n, f)\rangle$ (of norm possibly less than 1) such that

$$U_{T(p,n)}^{(p,n)} O U_{T(p,n)-1}^{(p,n)} O \ldots O U_0^{(p,n)} |0\rangle^{\otimes m} = |\phi_0(p, n, f)\rangle \otimes |0\rangle + |\phi_1(p, n, f)\rangle \otimes |1\rangle\,.$$

After the measure M, the result is 0 (reject) with probability $||\phi_0(p, n, f)||^2$ and 1 (accept) with probability $||\phi_1(p, n, f)||^2$. **The algorithm A is said to solve Simon's problem with bounded error probability** ϵ if it accepts any bijection with a probability of at least $1 - \epsilon$ and rejects every other function fulfilling Simon's promise with a probability of at least $1 - \epsilon$. By definition, the query complexity of A is the function T. In Section 3 we will prove the following lower bound.

Theorem 1. *If A is an algorithm which solves Simon's problem in $(\mathbb{Z}/p\mathbb{Z})^n$ with bounded error probability ϵ and query complexity T, then $T(p, n) = \Omega(n)$; more precisely,*

$$T(p,n) \geq \min\left(\frac{n}{4}, \frac{\log_2\left((2-4\epsilon)\frac{p^{n+3}}{p-1}\right) - 1}{2\log_2\left(\frac{p^3}{p-1}\right) + 2}\right).$$

Although it might not be self-evident that $T(p, n) = \Omega(n)$, this bound is actually in the expected range. Indeed, using $\frac{p^{n+3}}{p-1} \geq p^{n+2}$ and $\frac{p^3}{p-1} \leq 2p^2$, we get

$$T(p,n) \geq \min\left(\frac{n}{4}, \frac{\log_2(2-4\epsilon) + (n+2)\log_2 p - 1}{4 + 4\log_2 p}\right).$$

If we suppose that $\epsilon \leq \frac{1}{4}$ to simplify matters, we then obtain

$$T(p,n) \geq \min\left(\frac{n}{4}, (n+1)\frac{\log_2 p}{4\left(1+\log_2 p\right)}\right) \geq \frac{n}{8}.$$

For $p = 2$ we obtain the result presented in our preprint [10]: when n is large enough,

$$T(2,n) \geq \frac{n + 2 + \log_2(2-4\epsilon)}{8}.$$

As explained in the introduction, our proof of this theorem is based on the polynomial method. Lemma 1 below is the key observation on which this method relies. We state it using the formalism of [1]: if s is a partial function from $(\mathbb{Z}/p\mathbb{Z})^n$ to X and f a function from $(\mathbb{Z}/p\mathbb{Z})^n$ to X, $|\mathrm{dom}(s)|$ denotes the size of the domain of s, and we define:

$$I_s(f) = \begin{cases} 1 & \text{if } f \text{ extends } s \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 1 (*[3]*). *If A is an algorithm of query complexity T, then there is a set S of partial functions from $(\mathbb{Z}/p\mathbb{Z})^n$ to E such that, for all functions $f : (\mathbb{Z}/p\mathbb{Z})^n \to E$, the algorithm A accepts f with probability*

$$P_{p,n}(f) = \sum_{s\in S} \alpha_{p,n,s} I_s(f)$$

where, for every $s \in S$, we have $|\mathrm{dom}(s)| \leq 2T(p,n)$ and the $\alpha_{p,n,s}$ are real numbers.

Here is the reason why $P_{p,n}$ is considered to be a polynomial. Let $\Delta_{i,j}(f)$ be 1 if $f(i) = j$ and 0 otherwise. Then $I_s(f)$ is a monomial in the variables $(\Delta_{i,j}(f))$:

$$I_s(f) = \prod_{i\in\mathrm{dom}(s),\, j=s(i)} \Delta_{i,j}(f)$$

and $P_{p,n}$ is a polynomial in the $(\Delta_{i,j})$.

The goal is now to transform $P_{p,n}(f)$ into a low-degree polynomial of a single real variable. This is achieved in Proposition 1. We can then prove and apply our lower bound result on real polynomials (Lemma 5).

3. Lower bound proof

An algorithm for Simon's problem is only supposed to distinguish between the trivial subgroup and a hidden subgroup of cardinality p (we recall that p is a prime number). To establish our lower bound, we will nonetheless need to examine its behaviour on a black-box hiding a subgroup of arbitrary order (a similar trick is used in [1] and [14]). As a side remark, note that this 'generalized Simon problem' (finding an arbitrary hidden subgroup of $(\mathbb{Z}/p\mathbb{Z})^n$) can still be solved in $O(n)$ queries and bounded probability of error by essentially the same algorithm; see, for instance, [7].

From now on, we suppose that A is an algorithm that solves Simon's problem with probability of error bounded by $\epsilon < \frac{1}{2}$ and query complexity T. Moreover, $P_{p,n}(f) = \sum_{s\in S} \alpha_{p,n,s} I_s(f)$, as given by Lemma 1, and $|\mathrm{dom}(s)|$ is at most $2T(p,n)$ for each s in the sum.

For $0 \leq d \leq n$ and $D = p^d$, let $Q_{p,n}(D)$ be the probability that A accepts f when f is chosen uniformly at random among the functions from $(\mathbb{Z}/p\mathbb{Z})^n$ to X hiding a subgroup of $(\mathbb{Z}/p\mathbb{Z})^n$ of order D. If we denote by X_D the set of functions hiding a subgroup of order D, then we have:

$$Q_{p,n}(D) = \frac{1}{|X_D|} \sum_{f\in X_D} P_{p,n}(f).$$

Of course, $Q_{p,n}(D)$ is only defined for some integer values of D and it can be extended in many different ways. By abuse of language, we will say that $Q_{p,n}$ is a polynomial of degree δ if it can be interpolated by a polynomial of degree δ.

The point of this definition is that we have a bound on some values of $Q_{p,n}$, and a gap between two of them. Namely, we have:

1. for any integer $d \in [0; n]$, $0 \leq Q_{p,n}(p^d) \leq 1$ (this number is a probability), and
2. $Q_{p,n}(1) \geq 1 - \epsilon$ and $Q_{p,n}(p) \leq \epsilon$, hence $|Q'_n(x_0)| \geq \frac{1-2\epsilon}{p-1} > 0$ for some $x_0 \in [1; p]$.

By Lemma 1, we have

$$Q_{p,n}(D) = \sum_{s\in S} \left(\frac{\alpha_s}{|X_D|} \sum_{f\in X_D} I_s(f) \right).$$

Hence

$$Q_{p,n}(D) = \sum_{s\in S} \alpha_s Q^s_{p,n}(D) \tag{1}$$

where $Q^s_{p,n}(D)$ is the probability that a random function f hiding a subgroup of order D extends s. We now prove that $Q_{p,n}$ is a low-degree polynomial. By (1), it suffices to bound the degree of $Q^s_{p,n}$. Let us start by counting subgroups:

Lemma 2. *Let n and k be non-negative integers. The group $(\mathbb{Z}/p\mathbb{Z})^n$ has exactly $\beta_p(n,k)$ distinct subgroups of order p^k, where:*

$$\beta_p(n,k) = \prod_{0\le i<k} \frac{p^{n-i}-1}{p^{k-i}-1}.$$

Proof. We look at $(\mathbb{Z}/p\mathbb{Z})^n$ as a vector space over the field $\mathbb{Z}/p\mathbb{Z}$: from this point of view, the subgroups are the subspaces. We start by counting the number of free k-tuples of vectors. For the first v_0, we can choose anything but 0, so there are p^n-1 choices. For the second vector v_1 we can choose any element not in the subspace generated by v_0; p^n-p possibilities remain. For the third vector, any linear combination of v_0 and v_1 is forbidden: there are p^2 of them. In general, the number of free k-tuples of vectors is $\alpha_p(n,k) = \prod_{0\le i<k}\left(p^n-p^i\right)$. Each subspace of dimension k can be generated by $\alpha_p(k,k)$ different k-tuples, so the total number of subspaces of dimension k is

$$\frac{\alpha_p(n,k)}{\alpha_p(k,k)} = \prod_{0\le i<k} \frac{p^{n-i}-1}{p^{k-i}-1}.$$

Note that this formula is correct even if $k>n$, in which case $\alpha_p(n,k)=0$. □

Proposition 1. *The polynomial $Q_{p,n}$ is of degree at most $2T(p,n)$.*

By (1), it suffices to show that, for all partial functions $s : (\mathbb{Z}/p\mathbb{Z})^n \to E$ such that $|\mathrm{dom}(s)| \le 2T(p,n)$, the probability $Q^s_{p,n}(D)$ that a random function f hiding a subgroup of order D extends s is a polynomial in D of degree at most $2T(p,n)$. So, let s be such a partial function. We will proceed in three steps: we first examine the case where s is a constant function, then the case where s is injective, and finally the general case.

Lemma 3. *If the partial function $s : (\mathbb{Z}/p\mathbb{Z})^n \to E$ is constant, then the degree of $Q^s_{p,n}(D)$ is at most $\log_p |H_s|$, where H_s is the subgroup of $(\mathbb{Z}/p\mathbb{Z})^n$ generated by $\mathrm{dom}(s)$.*

Proof. Let us recall that, according to our notations, $D=p^d$. Note that $\mathrm{dom}(s)=\{a_i/i=1\dots k\}$ with $k=|\mathrm{dom}(s)|$, the a_is being all different, of course. Moreover, we will suppose, without loss of generality, that $a_1=0$. Let H_s be the subgroup generated by $\mathrm{dom}(s)$ and $D_s=p^{d_s}$ its order. A function f hiding a subgroup H extends s if and only if $H_s\subseteq H$ and $f(a_1)=s(a_1)$. Since E, the possible range for f, is of size p^n, we have $Q^s_{p,n}(D)=\frac{\lambda(D,s)}{p^n}$, where $\lambda(D,s)$ is the proportion, among the subgroups of order D, of those containing $\mathrm{dom}(s)$ or, equivalently, H_s. The number of subgroups of order D containing H_s is equal to the number of subgroups of order $\frac{D}{D_s}$ of $(\mathbb{Z}/p\mathbb{Z})^n/H_s$, which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{n-d_s}$; so there are $\beta(n-d_s,d-d_s)$ of them. We then have

$$Q^s_{p,n}(D) = \frac{1}{p^n}\frac{\beta(n-d_s,d-d_s)}{\beta(n,d)} = \frac{1}{p^n}\prod_{0\le i<d_s}\frac{p^{d-i}-1}{p^{n-i}-1} = \frac{1}{p^n}\prod_{0\le i<d_s}\frac{\frac{D}{p^i}-1}{p^{n-i}-1},$$

which is a polynomial in D of degree d_s. □

Lemma 4. *If the partial function $s : (\mathbb{Z}/p\mathbb{Z})^n \to E$ is injective, then the degree of $Q^s_{p,n}(D)$ is at most $|\mathrm{dom}(s)|$.*

Proof. Likewise, we write $D=p^d$ and $\mathrm{dom}(s)=\{a_i/i=1\dots k\}$ with $k=|\mathrm{dom}(s)|$. A function f hiding a subgroup H extends s if and only if the a_is lie in distinct cosets of H, and f takes appropriate values on these cosets. So $Q^s_{p,n}(D)=\nu^s_{p,n}(D)\lambda^s_{p,n}(D)$, where $\lambda^s_{p,n}(D)$ is the probability for a subgroup H of order D of containing none of the $a_i-a_j (i\neq j)$ and $\nu^s_{p,n}(D)$ is the probability of extending s for a function f hiding a subgroup H of order D that does not contain any of the $a_i-a_j (i\neq j)$.

First we compute $\nu^s_{p,n}(D)$. For each subgroup H of order D that does not contain any of the $a_i-a_j (i\neq j)$, there are $p^n(p^n-1)\dots(p^n-p^{n-d}+1)$ possible functions f: choose a different value for each coset of H. Among these functions, the number of those that extend s is $(p^n-k)(p^n-k-1)\dots(p^n-p^{n-d}+1)$: choose a value for each coset not containing any a_i. So $\nu^s_{p,n}(D)=\frac{(p^n-k)!}{(p^n)!}$.

The probability $\lambda^s_{p,n}(D)$ is equal to $1-\mu^s_{p,n}(D)$, where $\mu^s_{p,n}$ is the probability for a subgroup H of order D of containing some a_i-a_j for some $i\neq j$.

By the inclusion–exclusion formula, we can expand $\lambda^s_{p,n}(D)$ as follows:

$$\lambda^s_{p,n}(D) = 1 - \left[\begin{array}{l} \displaystyle\sum_{i\neq j} \Pr(a_i - a_j \in H) \\ - \displaystyle\sum_{\substack{i_1\neq j_1\\ i_2\neq j_2\\ \{i_1;j_1\}\neq\{i_2;j_2\}}} \Pr(a_{i_1} - a_{j_1} \in H \wedge a_{i_2} - a_{j_2} \in H) \\ + \cdots \\ - \cdots \\ \vdots \\ + \Pr(\forall i \neq j\ a_i - a_j \in H) \end{array}\right].$$

By Lemma 3, each term in this sum is a polynomial in D of degree at most d', where the order of the subgroup generated by the $(a_i - a_j)$s is $p^{d'}$. Since $a_i - a_j$ is always in the subgroup generated by the $(a_i - a_1)$s, we have $d' \leq |\mathrm{dom}(s)|$. □

Proposition 1 can now be proven. The partial function s is defined by conditions of the form:

$$\begin{cases} s(a^1_1) = s(a^1_2) = \cdots = s(a^1_{k_1}) = b_1 \\ s(a^2_1) = s(a^2_2) = \cdots = s(a^2_{k_2}) = b_2 \\ \qquad\qquad \vdots \\ s(a^l_1) = s(a^l_2) = \cdots = s(a^l_{k_l}) = b_l \end{cases}$$

with $b_1, \ldots, b_l$ all different. In the same way as before, we will suppose, without loss of generality, that $a^1_1 = 0$. Furthermore, since $f(a^j_i) = f(a^j_1)$ is equivalent to $f(a^j_i - a^j_1) = f(0)$ (i.e., a^j_i and a^j_1 are in the same coset of H), we can remove each a^j_i, for $i, j > 1$, from $\mathrm{dom}(s)$ and replace them by adding the point $a^j_i - a^j_1$ to $\mathrm{dom}(s)$ associated with the value b_1. The number of conditions does not increase. It may happen that s was already defined on one of these entries and that our new definition is contradictory. In that case, there is simply no subgroup-hiding function f extending s, so $Q^s_{p,n}$ is simply the null polynomial and we are done. We will therefore consider only conditions of the form:

$$\begin{cases} s(0) = s(a^1_2) = \cdots = s(a^1_{k_1}) = b_1 \\ \qquad s(a^2) = b_2 \\ \qquad\quad \vdots \\ \qquad s(a^l) = b_l \end{cases}$$

with $k_1 + l \leq |\mathrm{dom}(s)|$.

The probability $Q^s_{p,n}(D)$ that a function f hiding a subgroup of order D extends s is the probability Q_1 that f satisfies $f(0) = f(a^1_2) = \cdots = f(a^1_{k_1}) = b_1$ times the probability Q_2 that f extends s given that $f(0) = f(a^1_2) = \cdots = f(a^1_{k_1}) = b_1$. We have already computed the first probability in Lemma 3: this is the case where s is constant. Let H' be the subgroup generated by the a^1_is. This group is of order $D' = p^{d'}$, where $d' \leq k_1 - 1$. Then

$$Q_1 = \frac{1}{p^n} \prod_{0\leq i<d'} \frac{p^{d-i} - 1}{p^{n-i} - 1} = \frac{1}{p^n} \prod_{0\leq i<d'} \frac{\frac{D}{i} - 1}{p^{n-i} - 1}.$$

Q_1 is thus a polynomial in D of degree at most $d' \leq k_1 - 1$. Let us now define s' on G/H' as the quotient of s if it exists (if not, this means again that $Q^s_{p,n}$ is the null polynomial, and we are done). If f satisfies $f(0) = f(a^1_2) = \cdots = f(a^1_{k_1}) = b_1$, then we can define f' on G/H' as the quotient of f; the condition 'f extends s and hides a subgroup of order D' is equivalent to 'f' extends s' and hides a subgroup of order D/D''. Since s' is defined by the condition $s'(H') = b_1, s'(a^2 + H') = b_2, \ldots, s'(a^l + H') = b_l$ and is injective, Lemma 4 tells us

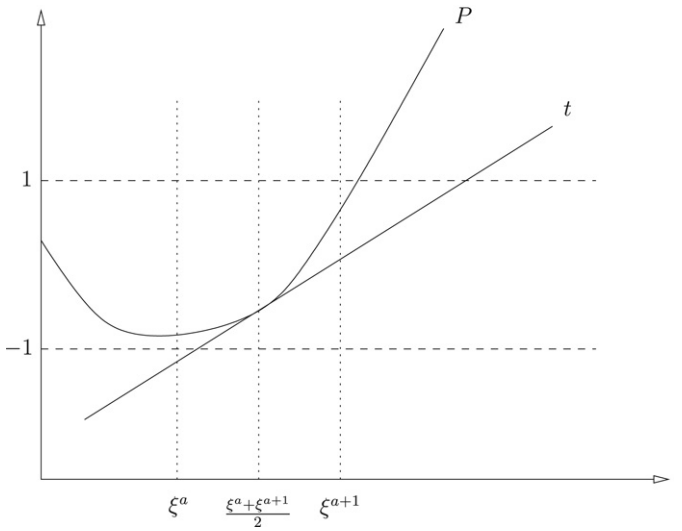

Fig. 1. The graph of P and a tangent.

that $Q_2 = Q^{s'}_{p,n}(D/D')$ is a polynomial in D of degree at most l. Hence, $Q^s_{p,n}(D)$ is a polynomial in D of degree at most $(k_1 - 1) + l \leq |\mathrm{dom}(s)| \leq 2T$.

Now that we have an upper bound on the degree of Q, let us find a lower bound. For this purpose, the following analogue of the lemmas of Paturi [17] and Nisan–Szegedy [16] will help.

Lemma 5. *Let $c > 0$ and $\xi > 1$ be constants and let P be a real polynomial with the following properties:*

1. *for any integer $0 \leq i \leq n$, we have $\left|P(\xi^i)\right| \leq 1$;*
2. *for some real number $1 \leq x_0 \leq \xi$, we have $\left|P'(x_0)\right| \geq c$.*

Then $\deg(P) = \Omega(n)$ *and, more precisely,*

$$\deg(P) \geq \min\left(\frac{n}{2}, \frac{\log_2\left(\xi^{n+3}c\right) - 1}{\log_2\left(\frac{\xi^3}{\xi-1}\right) + 1}\right).$$

Proof. Let d be the degree of P. If $d \geq n/2$, then there is nothing to prove, so we may and we will assume that $d \leq \frac{n}{2}$. The polynomials P' and P'' are, respectively, of degree $d-1$ and $d-2$, so there exists an integer $a \in [n - 2d + 2; n - 1]$ such that P'' has no real root in $\left(\xi^a; \xi^{a+1}\right)$, and P' has no root whose real part is in this same interval.

In the first part of the proof we upper bound $\left|P'\left(\frac{1+\xi}{2}\xi^a\right)\right|$ using the fact that $\frac{1+\xi}{2}\xi^a$ is the middle of the interval $\left(\xi^a; \xi^{a+1}\right)$ where P' is monotone. In the second part of the proof we lower bound $\left|P'\left(\frac{1+\xi}{2}\xi^a\right)\right|$ with a negative exponential of d, using the fact that P' has no root whose real part is in $\left(\xi^a; \xi^{a+1}\right)$. Both parts together give us the lemma.

First we prove that

$$\left|P'\left(\frac{1+\xi}{2}\xi^a\right)\right| \leq \frac{4}{\xi^a(\xi-1)}.$$

The polynomial P is either convex or concave on the interval $\left(\xi^a; \xi^{a+1}\right)$, for P'' has no root in it. Suppose it is convex and consider the tangent t to P at the middle point of the interval (see Fig. 1). The maximal variation of t on the interval $\left(\frac{\xi^a+\xi^{a+1}}{2}; \xi^{a+1}\right)$ is from -1 to 1 or from 1 to -1 and so

$$\left|P'\left(\frac{1+\xi}{2}\xi^a\right)\right| \leq \frac{2}{\frac{\xi^{a+1}-\xi^a}{2}} = \frac{4}{\xi^a(\xi-1)}.$$

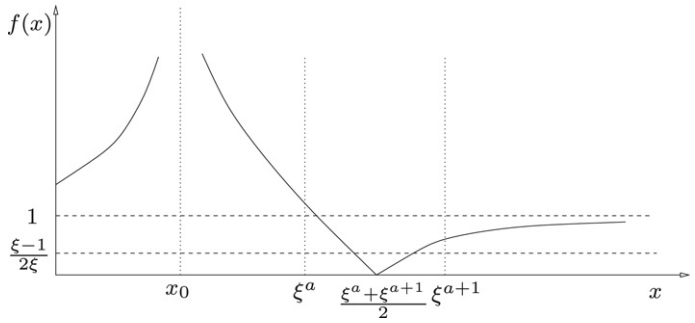

Fig. 2. The graph of f.

If P is concave, then considering the maximal variation of t on the interval $\left(\xi^a; \frac{\xi^a+\xi^{a+1}}{2}\right)$ proves the above inequality.

We therefore have

$$\left|\frac{P'\left(\frac{1+\xi}{2}\xi^a\right)}{P'(x_0)}\right| \leq \frac{4}{c\xi^a(\xi-1)} \leq \frac{4}{c\xi^{n-2d+2}(\xi-1)}. \tag{2}$$

Now we prove the lower bound:

$$\left|\frac{P'\left(\frac{1+\xi}{2}\xi^a\right)}{P'(x_0)}\right| \geq \left(\frac{\xi-1}{2\xi}\right)^{d-1}. \tag{3}$$

Let us write $P'(X) = \lambda \prod_{i=1}^{d-1}(X-\alpha_i)$, where the α_is are real or complex numbers. We have the following equality:

$$\left|\frac{P'\left(\frac{1+\xi}{2}\xi^a\right)}{P'(x_0)}\right| = \prod_{i=1}^{d-1}\left|\frac{\frac{1+\xi}{2}\xi^a-\alpha_i}{x_0-\alpha_i}\right|. \tag{4}$$

We lower bound the function $f(x) = \left|\frac{\frac{1+\xi}{2}\xi^a-x}{x_0-x}\right|$. If $x \in \mathbb{R}\setminus\left(\{x_0\}\cup\left(\xi^a;\xi^{a+1}\right)\right)$, then $f(x) \geq \min(1, f(\xi^a), f(\xi^{a+1})) \geq \frac{\xi-1}{2\xi}$ (see Fig. 2). Remember that no root α_i of P' has its real part in $\left(\xi^a;\xi^{a+1}\right)$. We therefore have

$$f(\Re(\alpha_i)) \geq \frac{\xi-1}{2\xi}. \tag{5}$$

To lower bound $f(\alpha_i)$ we need to state a simple geometric fact. Let MBC be a triangle, M' the orthogonal projection of M onto (BC), and (d) the perpendicular bisector of $[BC]$.

If M is 'at the left of (d)', i.e., $MC \geq MB$, then of course $\frac{MC}{MB} \geq 1$. Let us suppose that M is 'at the right of (d)', i.e., $MC \leq MB$ (see Fig. 3). Since C is closer to the line (MM') than B, $\tan\alpha = MM'/BM' \leq \tan\beta = MM'/CM'$. Hence $\alpha \leq \beta$, and $\cos\alpha \geq \cos\beta$, i.e., $\frac{MC}{MB} \geq \frac{M'C}{M'B}$. Finally:

$$\frac{MC}{MB} \geq \min\left(1, \frac{M'C}{M'B}\right). \tag{6}$$

We apply this result to the points $M = \alpha_i$, $M' = \Re(\alpha_i)$, $B = x_0$ and $C = \frac{1+\xi}{2}\xi^a$. We obtain the inequality

$$\left|\frac{\frac{1+\xi}{2}\xi^a-\alpha_i}{x_0-\alpha_i}\right| \geq \min\left(1, \left|\frac{\frac{1+\xi}{2}\xi^a-\Re(\alpha_i)}{x_0-\Re(\alpha_i)}\right|\right)$$

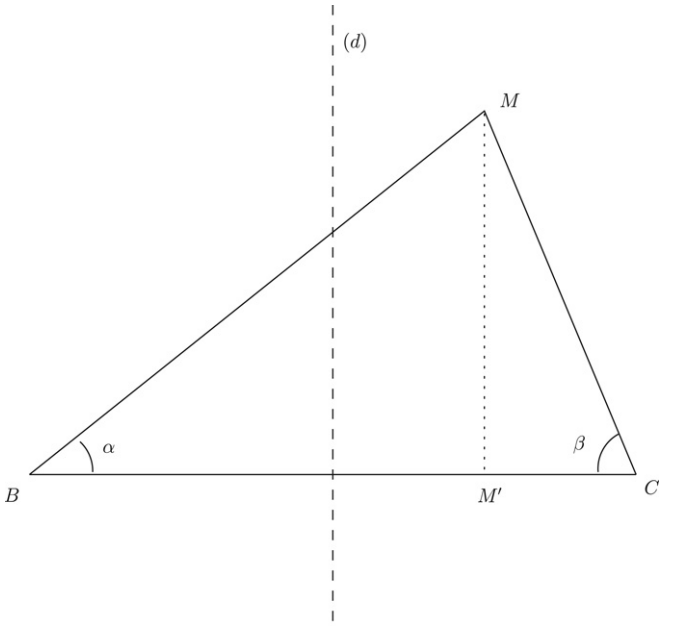

Fig. 3. The triangle MBC.

and thus $f(\alpha_i) \geq \frac{\xi-1}{2\xi}$ by (5). We conclude from (4) that

$$\left| \frac{P'\left(\frac{1+\xi}{2}\xi^a\right)}{P'(x_0)} \right| \geq \left(\frac{\xi-1}{2\xi}\right)^{d-1}.$$

Taking (2) into account, we finally obtain the inequality

$$\left(\frac{\xi-1}{2\xi}\right)^{d-1} \leq \frac{4}{c\xi^{n-2d+2}(\xi-1)}$$

hence

$$d \geq \frac{\log_2\left(\xi^{n+3}c\right)-1}{\log_2\left(\frac{\xi^3}{\xi-1}\right)+1}. \quad \square$$

We can now complete the proof of Theorem 1. Let A be our algorithm solving Simon's problem with bounded error probability ϵ and query complexity T. As pointed out before Lemma 2, the associated polynomial $Q_{p,n}$ satisfies $|Q'_n(x_0)| \geq 1-2\epsilon$ for some $x_0 \in [1,\xi]$ and $Q_{p,n}(\xi^i) \in [0,1]$ for any $i \in \{0,1,\ldots,n\}$. An application of Lemma 5 to the polynomial $P = 2Q_{p,n} - 1$ therefore yields the inequality

$$\deg(Q_{p,n}) \geq \min\left(\frac{n}{2}, \frac{\log_2\left((2-4\epsilon)\frac{p^{n+3}}{p-1}\right)-1}{\log_2\left(\frac{p^3}{p-1}\right)+1}\right).$$

Theorem 1 follows, since $\deg(Q_{p,n}) \leq 2T(p,n)$ by Proposition 1.

4. Abelian groups

In this section we give lower and upper bounds for the quantum query complexity of abelian hidden subgroup problems. As explained in the introduction, our bounds are optimal up to constant factors.

Let G be a finite abelian group, $\hat{G}$ its dual group, i.e., the group of its characters (see, for example, [7]). For each subgroup H of G, we denote $H^\perp$ the orthogonal of H, which is a subgroup of $\hat{G}$ consisting of those characters χ such

that $\chi(h) = 1$ for all $h \in H$. According to basic representation theory, $\hat{G}$ is isomorphic to G and, for all subgroups $H \leq G$, the index of $H^\perp$ in $\hat{G}$ is equal to the order of H.

The well-established method of Fourier sampling allows one, with one query to the black-box function, to pick a uniformly random element from the orthogonal of the hidden subgroup. In order to solve the hidden subgroup problem for G, this routine is run k times so as to generate k random elements $x_1, \ldots, x_k \in H^\perp$. The algorithm outputs the orthogonal of the group generated by $x_1, \ldots, x_k$. This output is correct if $x_1, \ldots, x_k$ generate all of $H^\perp$.

We will now show that this algorithm is optimal if we know when to stop, i.e., how many random elements should be picked in $H^\perp$. The following lemma implies that the query complexity of the cyclic subgroup problem is constant. Note that this fact is already pointed out (without proof) in [19]. We give the proof here for the sake of completeness.

Lemma 6. *For any integer $M \geq 1$, two random elements chosen uniformly and independently in $\mathbb{Z}/M\mathbb{Z}$ generate all of this group with probability at least $\frac{1}{2}$.*

Proof. Let us write $M = \prod_{i=1}^n p_i^{\alpha_i}$, where the p_is are distinct primes. Let $x_1, \ldots, x_k$ be k elements of $\mathbb{Z}/M\mathbb{Z}$. These elements generate all of $\mathbb{Z}/M\mathbb{Z}$ iff, for each $i \in \{1, \ldots, n\}$, there exists $j \in \{1, \ldots, k\}$ such that p_i does not divide x_j. Let X_i, for $i = 1, \ldots, n$, be the random variable which, to a random element x of $\mathbb{Z}/M\mathbb{Z}$, associates 0 if p_i divides x, and 1 otherwise. It is easily verified that the X_is are independent random variables (for instance, $\mathbb{P}[X_i = 0 \wedge X_j = 0] = \mathbb{P}[X_i = 0]\,\mathbb{P}[X_j = 0] = \frac{1}{p_i}\,\frac{1}{p_j}$ for $i \neq j$). The probability $\mathcal{P}(M, k)$ that the x_js generate $\mathbb{Z}/M\mathbb{Z}$ is therefore equal to the product over the p_is of the probabilities that p_i does not divide all of the x_js. Namely, $\mathcal{P}(M, k) = \prod_{i=1}^n (1 - p_i^{-k})$. Note that $\log_2 \mathcal{P}(M, k) = \sum_{i=1}^n \log_2(1 - p_i^{-k}) \geq -2\sum_{i=1}^n p_i^{-k}$. Let $\mathbb{P} = \{2, 3, 5, \ldots\}$ be the set of prime numbers and let $k_1 \in \mathbb{N}$ be such that

$$\sum_{p \in \mathbb{P}} p^{-k_1} \leq -\frac{\log_2\left(1 - \frac{1}{2}\right)}{2} = \frac{1}{2}.$$

Using the fact that $\sum_{n \in \mathbb{N}^*} n^{-2} = \frac{\pi^2}{6}$, it can easily be verified that $k_1 = 2$ is suitable. Then $\mathcal{P}(M, 2) \geq \frac{1}{2}$ and we are done. □

We recall that (following, for instance, [13]) the rank $r(G)$ of a group G is the minimal cardinality of a generating set of G. According to the fundamental theorem of finite abelian groups, G is isomorphic to $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_{r(G)}\mathbb{Z}$, where m_i divides m_{i-1} for every $i \in \{2, \ldots, r(G)\}$, and this decomposition is unique.

Proposition 2. *For any $\epsilon > 0$ there exists an integer k such that, for any finite abelian group G, $k.r(G)$ random elements chosen uniformly and independently in G generate all of this group with a probability of at least $1 - \epsilon$.*

Proof. Let us denote by $\mathcal{E}_n$ the supremum of the expectations of the number of random elements of G needed to generate G, taken over the groups G such that $r(G) \leq n$. We can assume that $G = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_{r(G)}\mathbb{Z}$, where $m_{r(G)} | \ldots | m_1$. To generate G we can proceed with the following two steps.

First we pick enough random elements $(x_1^1, \ldots, x_1^{r(G)}), \ldots, (x_k^1, \ldots, x_k^{r(G)})$ in G so that $x_1^1, \ldots, x_k^1$ generate $\mathbb{Z}/m_1\mathbb{Z}$; the expectation of k is at most $\mathcal{E}_1$. By Lemma 6, $\mathcal{E}_1$ is finite; we can very roughly bound it in the following way.

First pick two random elements in $\mathbb{Z}/m_1\mathbb{Z}$. With probability $p_{\leq 2}$ they generate $\mathbb{Z}/m_1\mathbb{Z}$ and with probability $p_{>2}$ they do not; when they fail to generate, just forget about them and renew the experiment with two new random elements. In the first case the expectation of the number of elements is 2 and in the second case it is at most $2 + \mathcal{E}_1$, so we have $\mathcal{E}_1 \leq 2p_{\leq 2} + (2 + \mathcal{E}_1)\, p_{>2}$. Clearly, $p_{\leq 2} + p_{>2} = 1$ and, according to Lemma 6, we have $p_{\leq 2} \geq \frac{1}{2}$. This shows that $\mathcal{E}_1 \leq 4$.

Then the subgroup generated by these elements contains some element $y = (y^1, \ldots, y^{r(G)})$ such that the order of y^1 is m_1. The rank of $G/\langle y \rangle$ is equal to $r(G) - 1$, since $G/\langle y \rangle$ is isomorphic to $\mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_{r(G)}\mathbb{Z}$. This isomorphism follows from the fact the classes of $e_2, \ldots, e_{r(G)}$ generate $G/\langle y \rangle$, where e_i denotes the element of G whose ith coordinate is equal to 1 and all other coordinates are equal to 0. We now pick enough random elements $x_{k+1}, \ldots, x_{k+l} \in G$ so that their images in $G/\langle y \rangle$ generate all of it; the expectation of l is, of course, at most $\mathcal{E}_{r(G)-1}$. Putting it together, we get $\mathcal{E}_{n+1} \leq \mathcal{E}_1 + \mathcal{E}_n$, so $\mathcal{E}_n \leq 4n$. By Markov's inequality, if we choose $\left\lfloor \frac{4}{\epsilon} \right\rfloor r(G)$ random elements in a group G, we generate all of this group with a probability of at least $1 - \epsilon$. □

We can now prove our main result.

Theorem 2. *The quantum query complexity of the hidden subgroup problem in a finite abelian group G is $\Theta(r(G))$.*

Proof. The upper bound is achieved with the standard method: one just applies Proposition 2 to the orthogonal of the hidden subgroup, which is isomorphic to a subgroup of G, using the fact that r is a non-decreasing function on finite abelian groups.

The lower bound of course comes from Theorem 1. Since, for every finite abelian group G, there is some prime p such that $(\mathbb{Z}/p\mathbb{Z})^{r(G)}$ is isomorphic to some subgroup of G, we need only to state that the hidden subgroup problem for a subgroup of G reduces correctly to the hidden subgroup problem for G. Indeed, let H be a subgroup of G and let $H + t_0, \ldots, H + t_k$ be the cosets of H in G, where $t_0 = 0$. If $\gamma : H \to X$ hides a subgroup of H, then we can define a function $\gamma' : G \to X \times \{t_i / 0 \leq i \leq k\}$ which hides the same subgroup. Namely, we define $\gamma'(x + t_i) = (\gamma(x), t_i)$ for $x \in H$. Moreover, a call to γ' uses just one call to γ, so we are done. □

Although this result seems to say nothing about non-abelian groups, for some of them lower bounds do follow from Theorem 2. Indeed, if G is a finite group and H an abelian subgroup of G, then the quantum query complexity of the hidden subgroup problem in G is lower bounded by $\Omega(r(H))$. For example, since the symmetric group $\mathfrak{S}_n$ contains $\lfloor n/2 \rfloor$ involutions with disjoint supports, the complexity of its hidden subgroup problem is at least as high as that of Simon's problem in dimension $\lfloor n/2 \rfloor$, that is, $\Omega(n)$. This lower bound is not very far away from the best known upper bound of $O(n \log(n))$, which follows from the $O(\log |G|)$ query complexity upper bound obtained by Ettinger, Høyer and Knill for arbitrary finite groups[2] [5]. There are simple examples of hidden subgroup problems for which the gap between the best known upper and lower bounds is much worse. In particular, for dihedral groups the best upper bound is again $O(\log |G|)$, but no non-constant lower bound is known.

Acknowledgements

Many thanks to Xavier Caruso, Yves de Cornulier and Joël Riou for useful help. Thanks also go to Frédéric Magniez and to the ICALP 2005 referees for bibliographical hints. Finally, the comments of the TCS referees have led to several improvements in the presentation of this paper.

References

[1] Scott Aaronson, Yaoyun Shi, Quantum lower bounds for the collision and the element distinctness problems, Journal of the ACM 51 (4) (2004) 595–605.
[2] Robert Beals, Quantum computation of Fourier transforms over symmetric groups, in: Proceedings of the 29th Annual ACM Symposium on the Theory of Computation, STOC, ACM Press, 1997, pp. 48–53.
[3] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, Ronald de Wolf, Quantum lower bounds by polynomials, Journal of the ACM 48 (4) (2001) 778–797.
[4] Gilles Brassard, Peter Høyer, An exact quantum polynomial-time algorithm for Simon's problem, in: Israel Symposium on Theory of Computing Systems, 1997, pp. 12–23.
[5] Mark Ettinger, Peter Høyer, Emanuel Knill, The quantum query complexity of the hidden subgroup problem is polynomial, Information Processing Letters 91 (1) (2004) 43–48.
[6] Lisa R. Hales, The Quantum Fourier Transform and Extensions of the Abelian Hidden Subgroup Problem, Ph.D. Thesis, UC Berkeley, 2002.
[7] Mika Hirvensalo, Quantum Computing (Natural Computing Series), SpringerVerlag, 2001.
[8] Peter Høyer, Conjugated operators in quantum algorithms, Physics Review A 59 (1999) 3280–3289.
[9] R. Jozsa, Quantum algorithms and the Fourier transform, Proceedings of the Royal Society of London Series A 454 (1998).
[10] Pascal Koiran, Vincent Nesme, Natacha Portier, A quantum lower bound for the query complexity of Simon's problem. http://www.arxiv.org/pdf/quant-ph/0501060.
[11] Pascal Koiran, Vincent Nesme, Natacha Portier, The quantum query complexity of the Abelian hidden subgroup problem, LIP Technical Report RR2005-17. http://perso.ens-lyon.fr/pascal.koiran.
[12] Greg Kuperberg, A subexponential-time quantum algorithm for the dihedral hidden subgroup problem, Quantum Physics e-Print Archive, 2003.
[13] Hans Kurzweil, Bernd Stellmacher, The Theory of Finite Groups, An Introduction, Universitext, Springer, 2004.

[2] This upper bound only applies to the problem of deciding whether a hidden subgroup is non-trivial. If one wishes to determine the subgroup, the query complexity upper bound is still polynomial in $\log |G|$ but of higher degree.

[14] Samuel Kutin, Quantum lower bound for the collision problem with small range, Theory of Computing 1 (2005) 29–36. http://theoryofcomputing.org.
[15] Michael A. Nielsen, Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[16] Noam Nisan, Mario Szegedy, On the degree of boolean functions as real polynomials, Comput. Complexity 4 (4) (1994) 301–313.
[17] Ramamohan Paturi, On the degree of polynomials that approximate symmetric boolean functions (preliminary version), in: STOC '92: Proceedings of the Twenty-fourth Annual ACM Symposium on Theory of Computing, 1992, pp. 468–474.
[18] Pierre Philipps, Bornes inférieures en calcul quantique : Méthode par adversaire vs. méthode des polynômes, Rapport de stage de DEA, effectué au LRI sous la direction de Frédéric Magniez, http://www.lri.fr/~magniez/stages-dea.html, 2003.
[19] Peter W. Shor, Polynomial-time algorithms for prime factorisation and discrete logarithms on a quantum computer, SIAM Journal on Computing 26 (5) (1997) 1484–1509.
[20] David R. Simon, On the power of quantum computation, SIAM Journal on Computing 26 (5) (1997) 1474–1483.